

Product Description

Model EIR618-2SFP-T

Documentation Number: EIR618-2SFP-T_5107m



707 Dayton Road -- P.O. Box 1040 -- Ottawa, IL 61350 USA
Phone (815) 433-5100 -- General Fax (815) 433-5105

Phone (815) 433-5100 -- **General Fax** (815) 433-5105

Website: www.bb-elec.com

Sales e-mail: orders@bb-elec.com -- **Fax** (815) 433-5109

Technical Support e-mail: support@bb.elec.com -- **Fax** (815) 433-5104

European Headquarters

B&B Electronics

Westlink Commercial Park -- Oranmore, Co. Galway, Ireland

Phone +353 91-792444 -- **Fax** +353 91-792445

Website: www.bb-europe.com

Sales e-mail: sales@bb-europe.com

Technical Support e-mail: support@bb-europe.com

B&B Electronics Mfg. Co. Inc. -- December 2007

Eighteen Port Managed Industrial Ethernet Switches

User Manual



Notice

The contents of this manual are based on the firmware, kernel version, and hardware version listed below.

Firmware Version	V1.07
Kernel Version	V2.07
Hardware Version	-----

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Introduction	1
Features	1
Software Specification.....	3
Package Contents	5
Hardware Description	6
Physical Dimension	6
Front Panel.....	6
Top View	7
LED Indicators.....	8
Ports	9
Cabling	11
Wiring the Power Inputs	14
Wiring the Fault Alarm Contact	15
Mounting Installation	16
DIN-Rail Mounting	16
Wall Mount Plate Mounting	18
Hardware Installation	19
Network Application	20

X-Ring Application.....	20
Coupling Ring Application	21
Dual Homing Application	22
Console Management.....	23
Connecting to the Console Port	23
Pin Assignment	23
Login in the Console Interface	24
CLI Management.....	25
Commands Level	26
Commands Set List	27
System Commands Set.....	27
Port Commands Set	30
Trunk Commands Set	32
VLAN Commands Set	33
Spanning Tree Commands Set	35
QOS Commands Set.....	38
IGMP Commands Set	38
Mac / Filter Table Commands Set.....	39
SNMP Commands Set	40
Port Mirroring Commands Set	42
802.1x Commands Set.....	43

TFTP Commands Set.....	45
SystemLog, SMTP and Event Commands Set.....	45
SNTP Commands Set.....	47
X-ring Commands Set.....	48
Web-Based Management	50
About Web-based Management	50
Preparing for Web Management.....	50
System Login.....	51
System Information	52
IP Configuration	52
DHCP Server – System configuration.....	54
DHCP Server – Client Entries	54
DHCP Server - Port and IP Bindings	55
TFTP - Update Firmware	56
TFTP – Restore Configuration	56
TFTP - Backup Configuration.....	57
System Event Log – Syslog Configuration.....	57
System Event Log - SMTP Configuration	58
System Event Log - Event Configuration	59

Fault Relay Alarm.....	61
SNTP Configuration	61
IP Security	64
User Authentication.....	65
Port Statistics	66
Port Control	67
Port Trunk.....	68
Aggregator setting	68
Aggregator Information.....	70
State Activity.....	70
Port Mirroring.....	72
Rate Limiting	73
VLAN configuration	74
VLAN configuration - Port-based VLAN	74
802.1Q VLAN	77
Rapid Spanning Tree	80
RSTP - System Configuration	80
RSTP - Port Configuration.....	81
SNMP Configuration	83
System Configuration	83

Trap Configuration.....	84
SNMPV3 Configuration	85
QoS Configuration.....	88
QoS Policy and Priority Type	88
Port-based Priority.....	89
COS Configuration	90
TOS Configuration.....	90
IGMP Configuration.....	90
X-Ring	92
Security	94
802.1X/Radius Configuration	94
MAC Address Table	97
Factory Default.....	99
Save Configuration.....	100
System Reboot.....	100
Trouble shooting.....	101
Technical Specification.....	102

Introduction

This managed industrial switch comes equipped with a proprietary redundant network protocol—X-Ring which provides an easy way to establish a redundant Ethernet network. With ultra high-speed recovery time (less than 300 ms) and a long MTBF (Mean Time Between Failures) the industrial switch will continue to operate until a Gigabit network infrastructure has been established, without requiring extra upgrade costs.

In addition to 10/100/1000Base-TX fast Ethernet ports, the switch has SFP (mini-GBIC) ports. Traditional RJ-45 ports can be used for up linking short distance (less than 100 m) wide-band paths, while the SFP slots can be used for the application of wideband uploading and long distance transmissions adding flexibility

Features

- System Interface/Performance
 - RJ-45 ports support Auto MDI/MDI-X Function
 - SFP (mini-GBIC) supports 100/1000 Dual Mode
 - Store-and-Forward Switching Architecture
 - Back-plane (Switching Fabric): 7.2Gbps
 - 1Mbits Packet Buffer
 - 8K MAC Address Table
 - Wide Operating Temperature (-40°C to 75°C)*
- Case/Installation
 - IP-30
 - DIN-Rail and Panel Mount
- Power Supply
 - Wide Range Redundant Power Design
 - Reverse Polarity Protection
 - Current Overload Protection

- **Spanning Tree**
 - IEEE 802.1d Spanning Tree
 - IEEE 802.1w Rapid Spanning Tree
- **VLAN**
 - Port Based VLAN
 - 802.1 Q Tag VLAN
 - GVRP
- **X-Ring**
 - X-Ring, Dual Homing, Couple Ring, and Central Ring Topology
- **Port Trunk with LACP**
- **QoS (Quality of Service)**
 - IEEE 802.1p Class of Service
 - Four priority queues per port
 - Port Base, Tag Base and Type of Service Priority
- **Bandwidth Control**
 - Ingress Packet Filter and Egress Rate Limit
 - Broadcast/Multicast Packet Filter Control
- **Port Mirror: Monitor traffic in switched networks**
 - TX Packet only
 - RX Packet only
 - Both of TX and RX Packet
- **System Event Log**
 - System Log Server/Client
 - SMTP e-mail Alert
 - Relay Alarm Output System Events
- **Security**
 - Port Security : MAC address entries/filter
 - IP Security: IP address security management to prevent intrusion
 - Login Security: IEEE802.1X/RADIUS
- **SNMP Trap**
 - Cold Start, Power status
 - Authentication failure
 - X-Ring topology change
 - Link up / Link down
- **IGMP with Query mode for Multi Media Application**

- TFTP Firmware Update and System Configure Restore and Backup
- Provides EFT protection 3,000 V_{DC} for power line
- Supports 6,000 V_{DC} Ethernet ESD protection

Software Specification

Management	<p>SNMP v1, v2c and v3 management</p> <p>Web interface management</p> <p>Telnet interface management</p> <p>Command Line Interface (CLI) management</p>
SNMP MIB	<p>RFC 1215 Trap</p> <p>RFC 1213 MIBII</p> <p>RFC 1157 SNMP MIB</p> <p>RFC 1493 Bridge MIB</p> <p>RFC 2674 VLAN MIB</p> <p>RFC 1643</p> <p>RFC 1757</p> <p>RSTP MIB</p> <p>Private MIB</p>
VLAN	<p>Port based VLAN</p> <p>IEEE802.1Q Tag VLAN (256 entries)/VLAN ID (up to 4k in number which can be assigned from 1 to 4096)</p> <p>GVRP (256 groups)</p> <p>Double Tag VLAN (Q in Q)*</p> <p>Private VLAN**</p>
Port Trunk with LACP	<p>LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members</p>
LLDP**	<p>Supports LLDP that allows the switch to advertise its identity and capabilities on the LAN</p>
Spanning tree	<p>IEEE802.1d spanning tree</p> <p>IEEE802.1w rapid spanning tree.</p>
X-Ring	<p>Supports X-Ring, Dual Homing, Couple Ring, and Central Ring</p>

	Provides redundant backup feature and the recovery time below 20ms
Quality of service	The quality of service determined by port, Tag and IPv4 Type of Service, IPv4/IPv6 Different Service
Class of service	Supports IEEE 802.1p class of service, per port provides 4 priority queues
Port Security	Supports 100 entries of MAC address for static MAC and another 100 for MAC filter
Port mirror	TX packet only RX packet only, Both of TX and RX packets
IGMP	Supports IGMP snooping v1, v2 and v3 Up to 256 multicast groups and IGMP query
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder
Login Security	Supports IEEE-802.1X Authentication/RADIUS
Bandwidth control	Supports ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K ~ 250Mbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast, Broadcast packet only and all of packets The packet filter rate can be set from 100k to 250Mbps
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown & power fail Alarm Relay current carry ability: 1A @ DC24V

SNMP Trap	Up to 3 Trap stations Cold start, Port link up, Port link down, Authentication Failure, Private Trap for power status, Power Alarm configuration, Fault Alarm, X-Ring topology change
DHCP	Provides DHCP Client/DHCP Server function
DNS	Provides DNS client feature Supports Primary and Secondary DNS Server
SNTP	Supports SNTP to synchronize system clock in Internet
Firmware update	TFTP firmware update TFTP backup and restore
Configuration upload and download	Supports binary configuration file for system quick installation

Package Contents

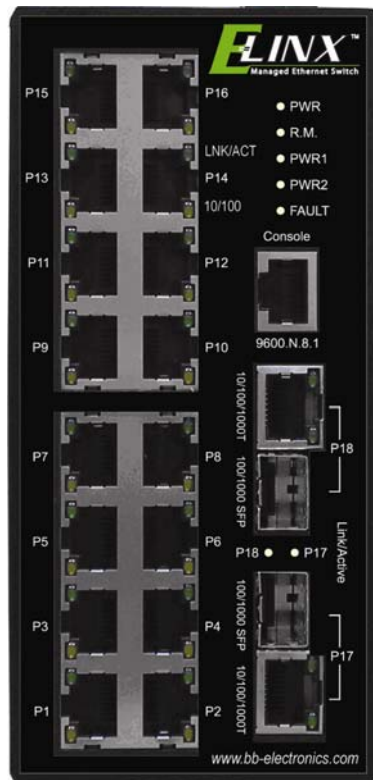
- Managed Industrial Switch x 1
- Pluggable Terminal Block x 1
- CD ROM with User manual x 1
- Mounting plate x 2
- Console Cable (RJ-45 to DB9-Female) x 1

Hardware Description

Physical Dimension

(W x D x H) 2.83 x 4.13 x 5.98 in (7.2mm x 10.5mm x 15.2 cm)

Front Panel



Front Panel of the industrial switch

Top View



Top Panel of the industrial switch

LED Indicators

LED	Status	Meaning
PWR	Green	Power On
	Off	No Power Inputs
R.M.	Green	The switch is the master of the X-Ring group
	Off	The industrial switch is not the master of the X-Ring group
PWR1	Green	Power Source 1 is Available
	Off	Power Source 1 is Unavailable
PWR2	Green	Power Source 2 is Available
	Off	Power Source 2 is Unavailable
Fault	Red	Power or port failure
	Off	Normal Operation
P1 through 16	Green (Upper LED)	Connected to network
	Blinking (Upper LED)	Network is active
	Off (Upper LED)	Not connected to network
	Yellow (Lower LED)	Full duplex
	Blinking (Lower LED)	Data packet collision
	Off (Lower LED)	Half duplex or not connected to network
P17/18 (10/100/1000T)	Green (Upper LED)	Connected to network

	Blinking (Upper LED)	Network is active
	Off (Upper LED)	Not connected to network
	Green (Lower LED)	The port is operating at 1000M
	Off (Lower LED)	The port is disconnected or operating at 10/100M
P17 /18 Link/Active (100/1000 SFP)	Green	SFP port is connected to network
	Blinking	Network is active
	Off	Not connected to network

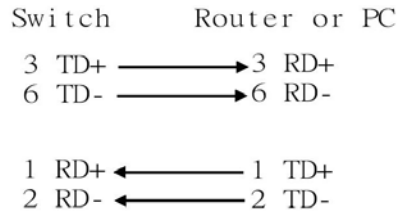
Ports

- **RJ-45 ports**

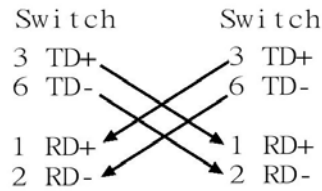
RJ-45 ports (Auto MDI/MDIX): The RJ-45 ports are auto-sensing for 10Base-T, 100Base-TX or 1000Base-T devices connections and Auto MDI/MDIX.

- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-



Straight Through Cable Schematic



Cross Over Cable Schematic

■ **Gigabit Copper/SFP (Mini-GBIC) combo port:**

The Industrial switch has auto-detecting Giga—UTP/STP/Fiber combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable. The SFP slots are for connecting to the network segment with single or multi-mode fiber. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications.

Note When an SFP module is inserted, the associated copper port is disabled.

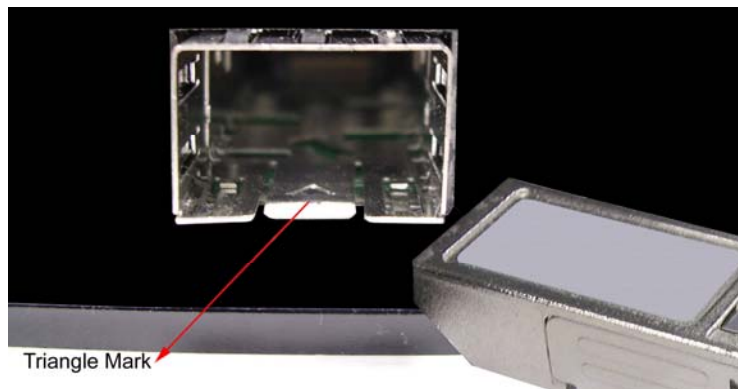
Cabling

Twisted-pair segment can be either unshielded twisted pair (UTP) or shielded twisted pair (STP) cabling. The cable between the link partner (switch, hub, workstation, etc.) and the converter must be less than 100 meters (328 ft.) long and comply with the IEEE 802.3ab 1000Base-T standard for Category 5e or above.

Single-mode fiber links must use 9/125 μ m single-mode fiber cable. Multi-mode fiber links must use 50/125 or 62.5/125 μ m multi-mode fiber cable. The small form-factor pluggable (SFP) is a compact optical transceiver

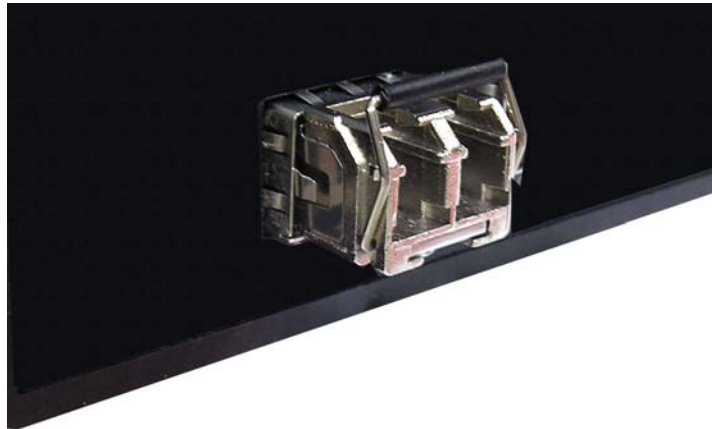
To connect the transceiver and LC cable, follow the steps shown below:

First, insert the transceiver into the SFP module. The triangle mark identifies bottom of the module.



Transceiver to the SFP module

Ensure the module is aligned correctly and then slide the module into the SFP slot until a click is heard.



Transceiver Inserted

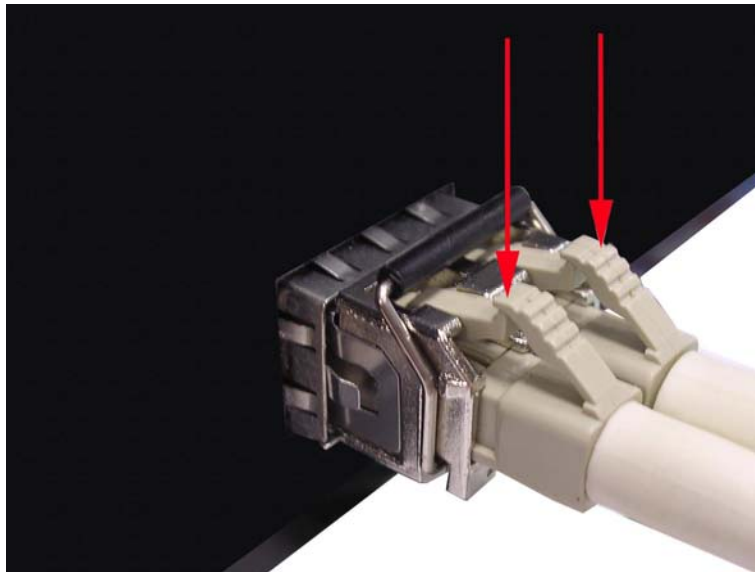
Insert the fiber cable into the transceiver.



LC connector to the transceiver

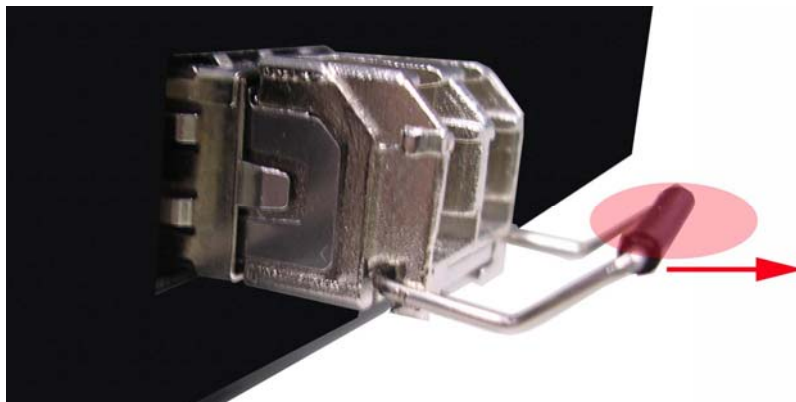
To remove the fiber cable from the transceiver, follow the steps shown below:

Press the upper side of the LC connector from the transceiver and pull it out to release.



Remove LC connector

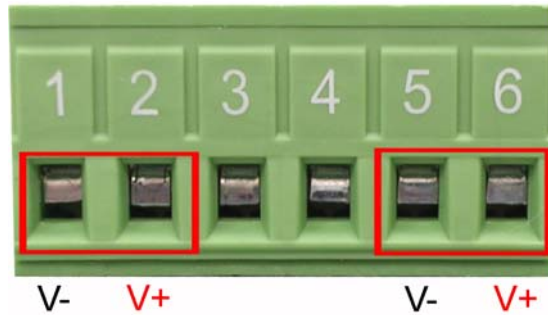
Push down the metal loop and pull the transceiver out by the plastic part.



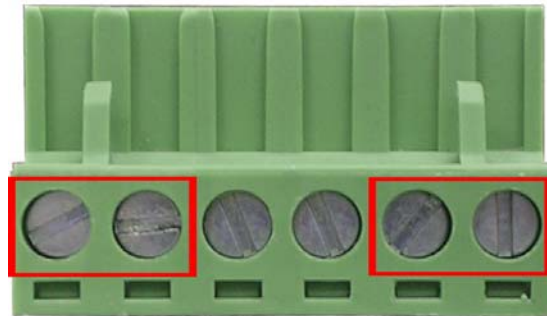
Pull out from the SFP module

Wiring the Power Inputs

Please follow the steps below to insert the power wire.



1. Insert the positive and negative leads into the V+ and V- contacts on the terminal block connector.



2. To tighten the wire-clamp screws.

Wiring the Fault Alarm Contact

The fault alarm contact is in the middle of terminal block connector.

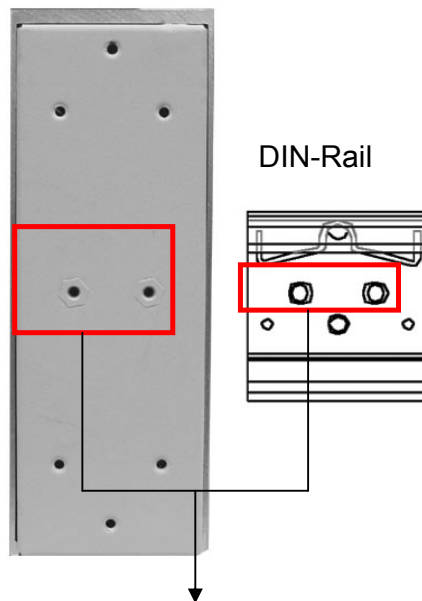


Note *Use 12 to 24 AWG wire.*

Mounting Installation

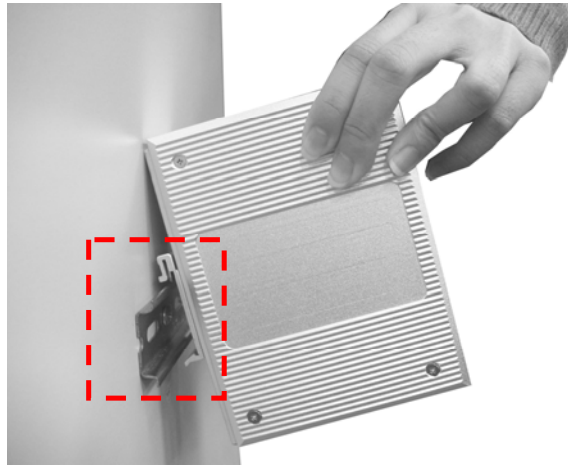
DIN-Rail Mounting

Rear Panel of
the switch

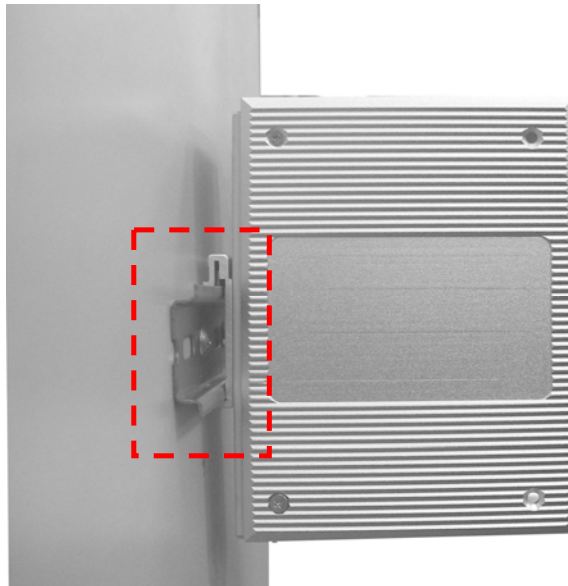


DIN-Rail

1. First, insert the top of the DIN-Rail clip into the track.



2. Then, lightly push into the track.

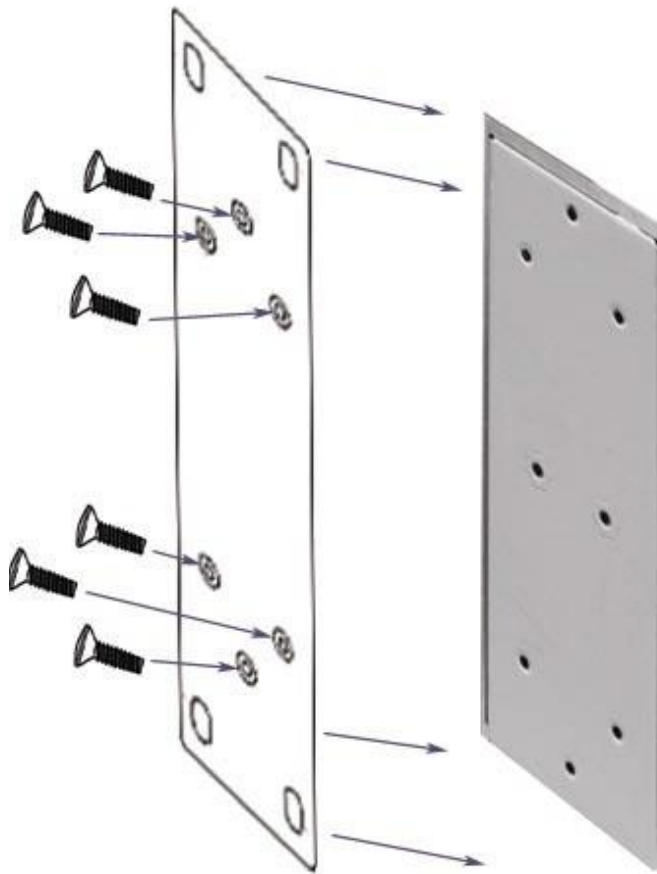


3. Ensure the DIN-Rail clip is tightly secured to the track.
4. To remove the industrial switch from the track, reverse steps above.

Panel Mounting

Follow the steps as below to mount the industrial switch with wall mount plate.

1. Remove the DIN-Rail from the industrial switch.
2. Place the panel mount plate on the rear panel.
3. Use the screws to attach the panel mount.
4. Use the hook holes at the corners of the plate to mount the switch to the.
To remove the wall mount plate, reverse steps above.



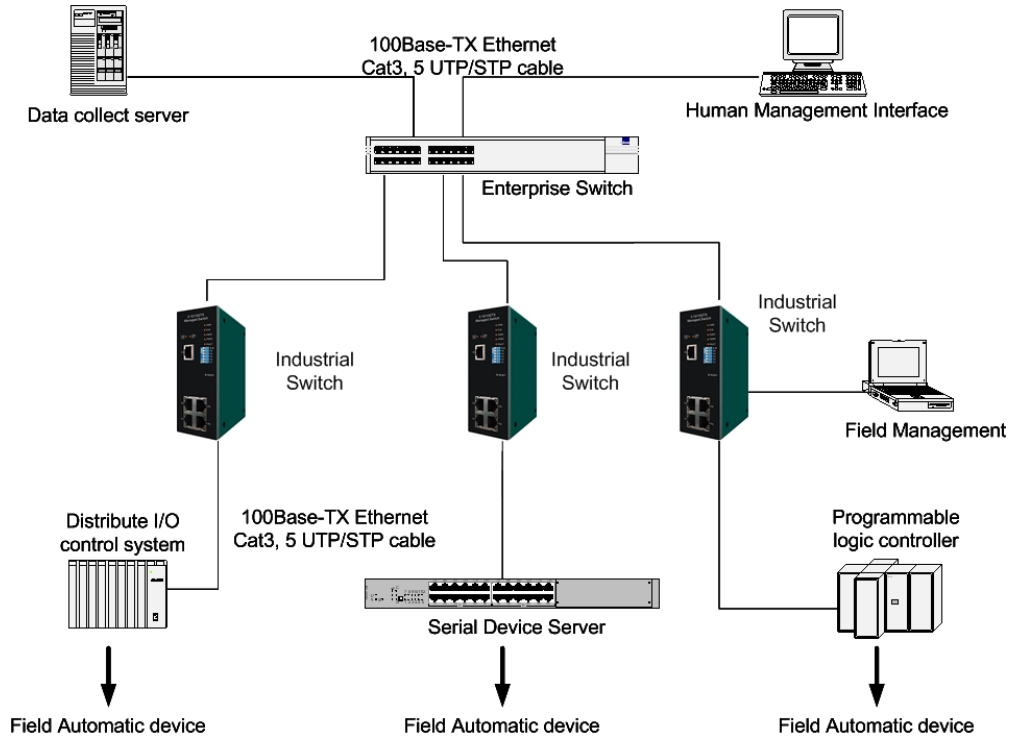
Hardware Installation

Installation Steps

1. Unpack the Industrial switch.
2. Ensure the DIN-Rail is tightly screwed to the Industrial switch. If not, refer to **DIN-Rail Mounting** section for DIN-Rail installation. To panel mount the Industrial switch, refer to **Panel Mounting** section.
3. Apply power to the switch (refer to the **Wiring the Power Inputs** section). The power LED will light.
4. Connect CAT 5 cables to the Industrial switch's RJ-45 ports and to the network devices

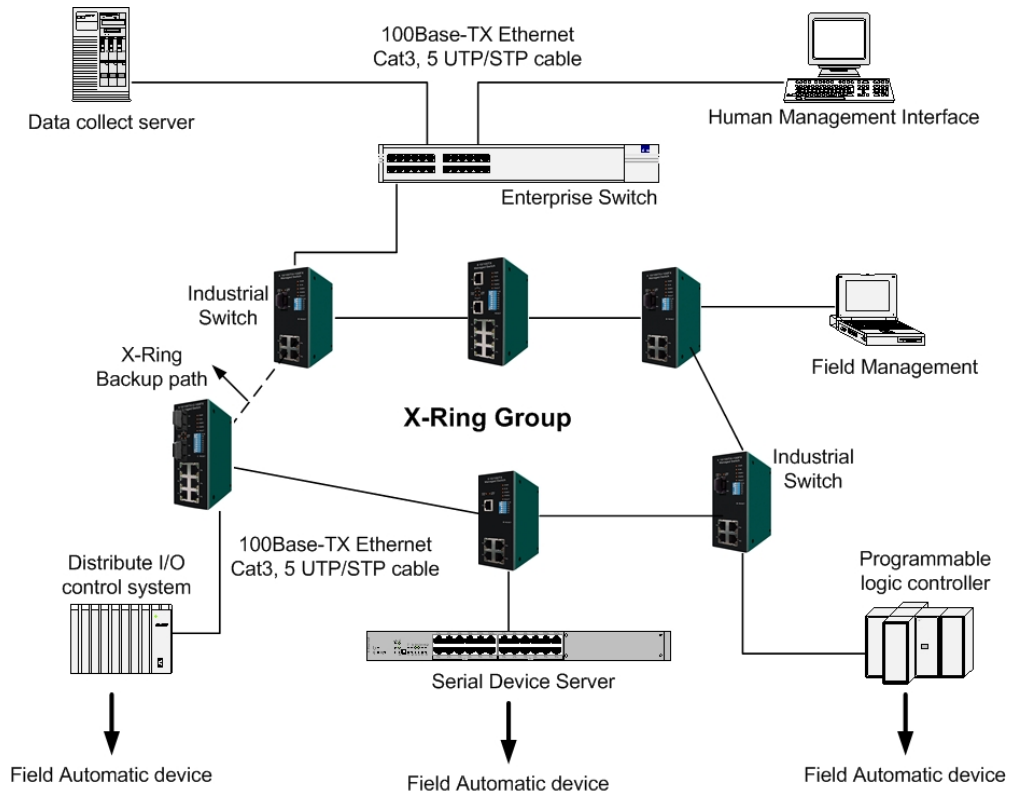
[NOTE] If the network devices do not support MID/MDIX, a crossover cable may be required.

Network Application



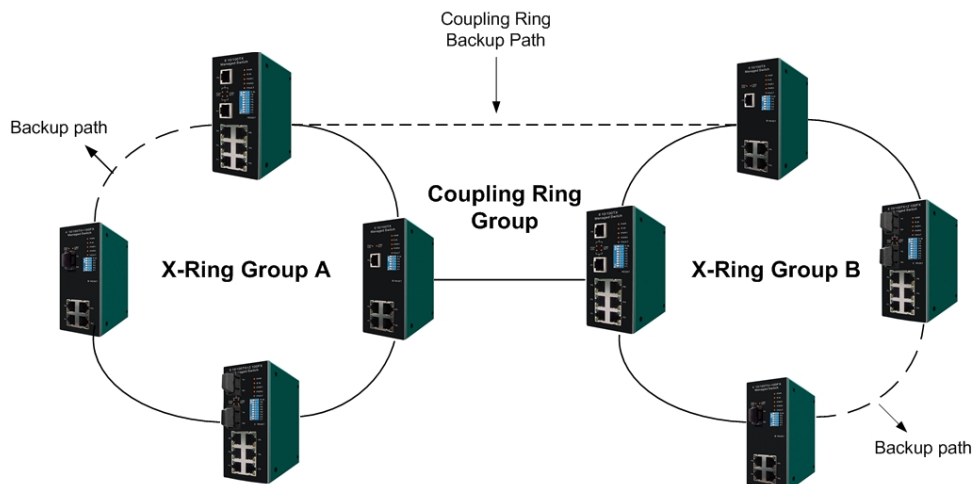
X-Ring Application

This switch incorporates the X-Ring Protocol to ensure network reliability and system restoration within 300 ms in the event of a connection failure. The X-Ring algorithm is similar to the spanning tree protocol (STP) algorithm but it has faster recovery time. The following figure below is an example of an X-Ring application.



Coupling Ring Application

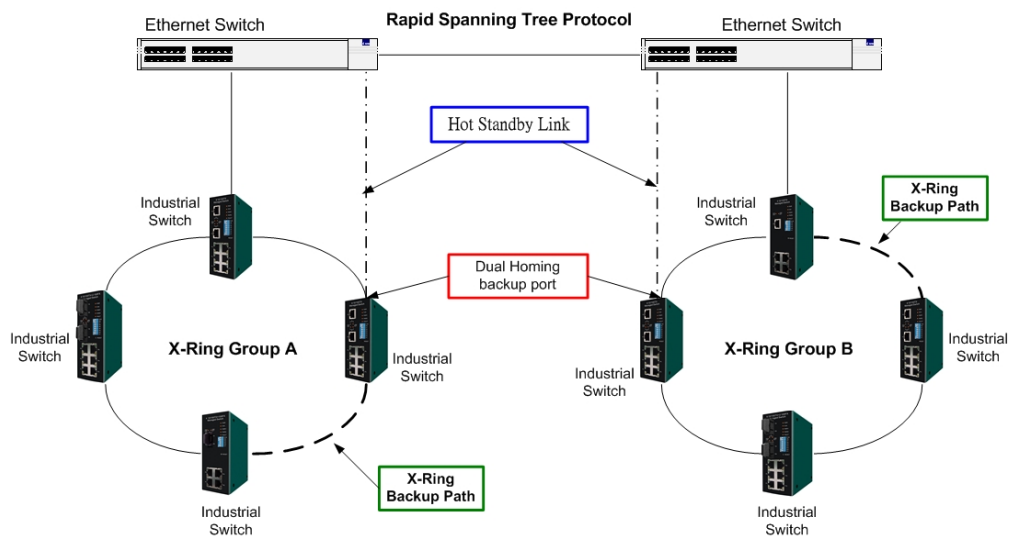
If the network has more than one X-Ring group, the coupling ring function is used to connect them and add redundancy. This ensures that transmissions between the two ring groups will not fail. The figure below is an example of the coupling ring application.



Dual Homing Application

The Dual Homing function is used to prevent a connection loss between the X-Ring group and the upper level/core switch. Assign a port in each X-ring group to be the Dual Homing ports. The Dual Homing function can only be used when the X-Ring function is active. Each X-Ring group can have one Dual Homing port. Note: The upper level switches must have RSTP enabled.

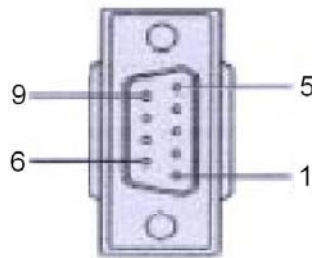
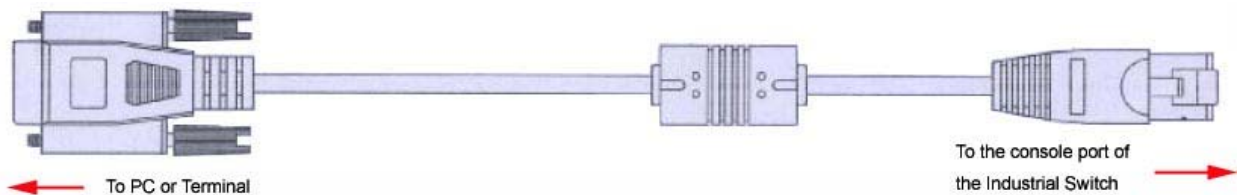
[NOTE] In Dual Homing application architecture, the upper level switches must enable the Rapid Spanning Tree protocol.



Console Management

Connecting to the Console Port

Attach the DB9 end to a PC or terminal and the RJ-45 end to the console port on the switch. The PC must have support a terminal emulation program.



DB 9-pin Female

Pin Assignment

DB9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC, run a terminal emulation program or Hyper Terminal, and configure the following communication parameters:

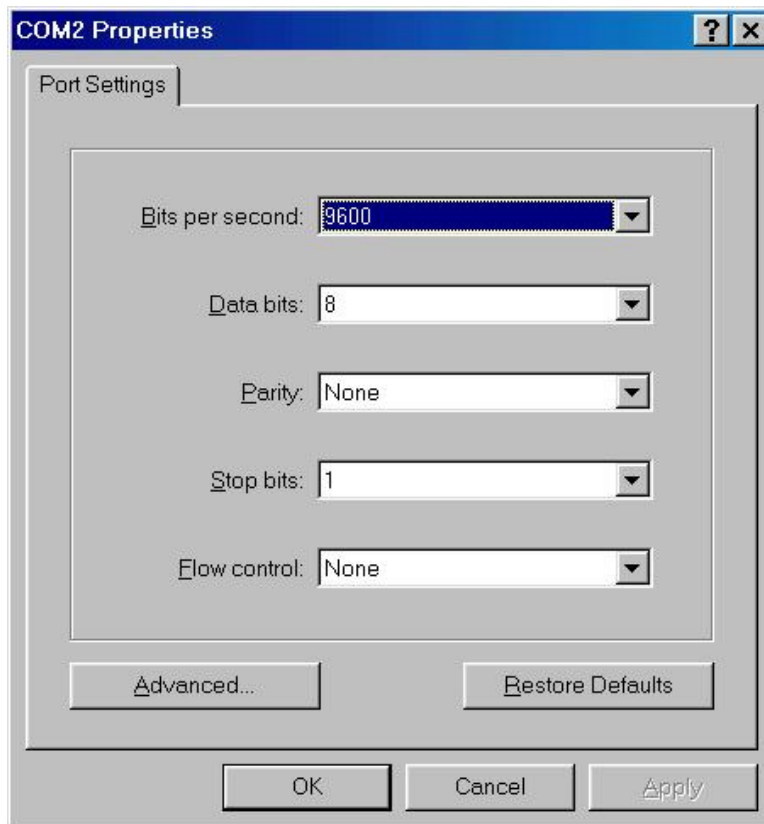
Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None



The settings of communication parameters

After entering the parameter, click '**OK**'. When the blank screen shows up, press Enter on the PC keyboard. A login screen will be displayed. Enter '**root**' for the User name and Password.

```
User Name :  
Password :
```

Console login interface

CLI Management

After you login to the system, you will see a command prompt. To enter CLI management interface, type '**enable**' and press enter.

```
switch>enable  
switch#_
```

CLI command interface

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit .	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to <ul style="list-style-type: none"> • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in User EXEC mode.	switch#	Enter disable to exit.	The privileged command is the advanced mode. Use this mode to <ul style="list-style-type: none"> • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure those parameters that are going to be applied to your switch.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit .	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface of	switch (config-if)#	To exit to global	Use this mode to configure parameters

	fast Ethernet command (with a specific interface) while in global configuration mode		configuration mode, enter exit . To exit to privileged EXEC mode, enter exit or end .	for the switch and Ethernet ports.
--	--	--	--	------------------------------------

Commands Set List

User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

System Commands Set

Commands	Level	Description	Example
show config	E	Show switch configuration	switch> show config
show terminal	P	Show console information	switch# show terminal
write memory	P	Save user configuration into permanent memory (flash rom)	switch# write memory
system name [System Name]	G	Configure system name	switch(config)# system name xxx
system location [System Location]	G	Set switch system location string	switch(config)# system location xxx
system description [System Description]	G	Set switch system description string	switch(config)# system description xxx

system contact [System Contact]	G	Set switch system contact window string	switch(config)# system contact xxx
show system-info	E	Show system information	switch> show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)# ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)# ip dhcp
show ip	P	Show IP information of switch	switch# show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)# no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)# reload
default	G	Restore to default	switch(config)# default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)# admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)# admin password xxxxxx
show admin	P	Show administrator information	switch# show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)# dhcpserver enable
Dhcpserver disable	G	Disable DHCP Server	switch(config)# no dhcpserver
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.100
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.200
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)# dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)# dhcpserver gateway 192.168.1.254
dhcpserver dnsip	G	Configure DNS IP for	switch(config)# dhcpserver dnsip

[DNS IP]		DHCP clients	192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)# dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)# interface fastEthernet 2 switch(config)# dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch# show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch# show dhcpserver clients
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch# show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)# no dhcpserver
security enable	G	Enable IP security function	switch(config)# security enable
security http	G	Enable IP security of HTTP server	switch(config)# security http
security telnet	G	Enable IP security of telnet server	switch(config)# security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)# security ip 1 192.168.1.55
show security	P	Show the information of IP security	switch# show security
no security	G	Disable IP security function	switch(config)# no security
no security http	G	Disable IP security of HTTP server	switch(config)# no security http
no security telnet	G	Disable IP security of telnet server	switch(config)# no security telnet

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)# interface fastEthernet 2
duplex [full half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)# interface fastEthernet 2 switch(config-if)# duplex full
speed [10 100 1000 auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)# interface fastEthernet 2 switch(config-if)# speed 100
no flowcontrol	I	Disable flow control of interface	switch(config-if)# no flowcontrol
security enable	I	Enable security of interface	switch(config)# interface fastEthernet 2 switch(config-if)# security enable
no security	I	Disable security of interface	switch(config)# interface fastEthernet 2 switch(config-if)# no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)# interface fastEthernet 2 switch(config-if)# bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast,	switch(config)# interface fastEthernet 2 switch(config-if)# bandwidth type

		multicast, and flooded unicast frame”	broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)# interface fastEthernet 2 switch(config-if)# bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)# interface fastEthernet 2 switch(config-if)# bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)# interface fastEthernet 2 switch(config-if)# bandwidth in 100
bandwidth out [Value]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)# interface fastEthernet 2 switch(config-if)# bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)# interface fastEthernet 2 switch(config-if)# show bandwidth
state [Enable Disable]	I	Use the state interface configuration command to specify the state mode of	switch(config)# interface fastEthernet 2 (config-if)# state Disable

		operation for Ethernet ports. Use the disable form of this command to disable the port.	
show interface configuration	I	show interface configuration status	switch(config)# interface fastEthernet 2 switch(config-if)# show interface configuration
show interface status	I	show interface actual status	switch(config)# interface fastEthernet 2 (config-if)# show interface status
show interface accounting	I	show interface statistic counter	switch(config)# interface fastEthernet 2 (config-if)# show interface accounting
no accounting	I	Clear interface accounting information	switch(config)# interface fastEthernet 2 switch(config-if)# no accounting

Trunk Commands Set

Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)# aggregator priority 22
aggregator activityport [Group ID] [Port Numbers]	G	Set activity port	switch(config)# aggregator activityport 2
aggregator group [GroupID] [Port-list] lACP workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a	switch(config)# aggregator group 1 1-4 lACP workp 2 or switch(config)# aggregator group 2 1,4,3 lACP workp 3

		comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)# aggregator group 1 2-4 nolacp or switch(config)# aggregator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch# show aggregator 1 or switch# show aggregator 2 or switch# show aggregator 3
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)# no aggregator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)# no aggregator group 2

VLAN Commands Set

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch# vlan database
Vlanmode [portbase 802.1q gvrp]	V	To set switch VLAN mode.	switch(vlan)# vlanmode portbase or switch(vlan)# vlanmode 802.1q

			or switch(vlan)# vlanmode gvrp
no vlan	V	No VLAN	Switch(vlan)# no vlan
Ported based VLAN configuration			
vlan port-based grpname [Group Name] grp-id [GroupID] port [PortNumbers]	V	Add new port based VLAN	switch(vlan)# vlan port-based grpname test grp-id 2 port 2-4 or switch(vlan)# vlan port-based grpname test grp-id 2 port 2,3,4
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)# show vlan 23
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)# no vlan group 2
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] vid [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)# vlan 8021q name test vid 22
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign an access link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)# vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag	V	Assign a hybrid link for VLAN by port; if the port belongs to a trunk	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or

[TaggedVID List]		group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)# vlan 8021q trunk 3 access-link untag 33
vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)# vlan 8021q trunk 3 trunk-link tag 2,3,6,99 or switch(vlan)# vlan 8021q trunk 3 trunk-link tag 3-20
vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)# show vlan 23
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)# no vlan group 2

Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)# spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)# spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives	switch(config)# spanning-tree max-age 15

		from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)# spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface	switch(config)# interface fastEthernet 2

		configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config-if)# stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)# interface fastEthernet 2 switch(config-if)# stp-path-priority 128
stp-admin-p2p [Auto True False]	I	Admin P2P of STP priority on this interface.	switch(config)# interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True False]	I	Admin Edge of STP priority on this interface.	switch(config)# interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True False]	I	Admin NonSTP of STP priority on this interface.	switch(config)# interface fastEthernet 2 switch(config-if)# stp-admin-non-s

			tp False
show spanning-tree	E	Displays a summary of the spanning-tree states.	switch> show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)# no spanning-tree

QOS Commands Set

Commands	Level	Description	Example
qos policy [weighted-fair strict]	G	Select QOS policy scheduling	switch(config)# qos policy weighted-fair
qos prioritytype [port-based cos-only tos-only cos-first tos-first]	G	Setting of QOS priority type	switch(config)# qos prioritytype
qos priority portbased [Port] [lowest low middle high]	G	Configure Port-based Priority	switch(config)# qos priority portbased 1 low
qos priority cos [Priority][lowest low middle high]	G	Configure COS Priority	switch(config)# qos priority cos 0 middle
qos priority tos [Priority][lowest low middle high]	G	Configure TOS Priority	switch(config)# qos priority tos 3 high
show qos	P	Displays the information of QoS configuration	Switch# show qos
no qos	G	Disable QoS function	switch(config)# no qos

IGMP Commands Set

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)# igmp enable
igmp-query auto	G	Set IGMP query to auto mode	switch(config)# igmp-query auto
igmp-query force	G	Set IGMP query to force mode	switch(config)# igmp-query force

show igmp configuration	P	Displays the details of an IGMP configuration.	switch# show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch# show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)# no igmp
no igmp-query	G	Disable IGMP query	switch# no igmp-query

Mac / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)# interface fastEthernet 2 switch(config-if)# mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)# mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch# show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch# show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch# show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)# interface fastEthernet 2 switch(config-if)# no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)# no mac-address-table filter hwaddr 000012348678

no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)# no mac-address-table
-----------------------------	----------	---	---

SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)# snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)# snmp system-location lab
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)# snmp system-contact where
snmp agent-mode [v1v2c v3 v1v2cv3]	G	Select the agent mode of SNMP	switch(config)# snmp agent-mode v1v2cv3
snmp community-strings [Community] right [RO/RW]	G	Add SNMP community string.	switch(config)# snmp community-strings public right rw
snmp-server host [IP address] community [Community-string] trap-version [v1 v2c]	G	Configure SNMP server host information and community string	switch(config)# snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)# snmpv3 context-name Test
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)# snmpv3 user test01 group G1 password AuthPW PrivPW

Password]			
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv AuthNoPriv AuthPriv] match-rule [Exact Prifix] views [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of SNMPV3 agent	switch(config)# snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1
snmpv3 mibview view [View Name] type [Excluded Included] sub-oid [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)# snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1
show snmp	P	Show SNMP configuration	switch# show snmp
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)# no snmp community-strings public
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)# no snmp-server 192.168.1.50
no snmpv3 user [User Name]	G	Remove specified user of SNMPv3 agent.	switch(config)# no snmpv3 user Test
no snmpv3 access context-name [Context Name]	G	Remove specified access table of SNMPv3 agent.	switch(config)# no snmpv3 access context-name Test group G1 security-level AuthPr

group [Group Name] security-level [NoAuthNoPriv AuthNoPriv AuthPriv] match-rule [Exact Prefix] views [Read View Name] [Write View Name] [Notify View Name]			iv match-rule Exact views V1 V1 V1
no snmp3 mibview view [View Name] type [Excluded Included] sub-oid [OID]	G	Remove specified mibview table of SNMPV3 agent.	switch(config)# no snmp3 mibview view V1 type Excluded sub-oid 1.3.6.1

Port Mirroring Commands Set

Commands	Level	Description	Example
monitor [RX TX Both]	I	Configure source port of monitor function	switch(config)# interface fastEthernet 2 switch(config-if)# monitor RX
monitor rx [Port ID]	G	Set RX destination port of monitor function	switch(config)# monitor rx 2
monitor tx [Port ID]	G	Set TX destination port of monitor function	switch(config)# monitor tx 3
show monitor	P	Show port monitor information	switch# show monitor
show monitor	I	Show port monitor information	switch(config)# interface fastEthernet 2 switch(config-if)# show monitor
no monitor	I	Disable source port of	switch(config)# interface

		monitor function	fastEthernet 2 switch(config-if)#no monitor
--	--	------------------	---

802.1x Commands Set

Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change	switch(config)# 8021x system nasid test1

		the NAS ID	
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)# 8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable reject accept	I	Use the 802.1x port state interface	switch(config)# interface fastethernet 3

<code>authorize]</code>		configuration command to set the state of the selected port.	<code>switch(config-if)#8021x portstate accept</code>
<code>show 8021x</code>	E	Displays a summary of the 802.1x properties and also the port states.	<code>switch>show 8021x</code>
<code>no 8021x</code>	G	Disable 802.1x function	<code>switch(config)#no 8021x</code>

TFTP Commands Set

Commands	Level	Description	Defaults Example
<code>backup flash:backup_cfg</code>	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	<code>switch(config)#backup flash:backup_cfg</code>
<code>restore flash:restore_cfg</code>	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	<code>switch(config)#restore flash:restore_cfg</code>
<code>upgrade flash:upgrade_fw</code>	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	<code>switch(config)#upgrade flash:upgrade_fw</code>

SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
<code>systemlog ip [IP address]</code>	G	Set System log server IP address.	<code>switch(config)# systemlog ip 192.168.1.100</code>

systemlog mode [client server both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Displays system log.	Switch> show systemlog
show systemlog	P	Show system log client & server information	switch# show systemlog
no systemlog	G	Disable systemlog function	switch(config)# no systemlog
smtp enable	G	Enable SMTP function	switch(config)# smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)# smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)# smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)# smtp account John
smtp password [password]	G	Configure authentication password	switch(config)# smtp password 1234
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)# smtp rcptemail 1 <u>Alert@test.com</u>
show smtp	P	Show the information of SMTP	switch# show smtp
no smtp	G	Disable SMTP function	switch(config)# no smtp
event device-cold-start [Systemlog SMTP Both]	G	Set cold start event type	switch(config)# event device-cold-start both
event authentication-failure [Systemlog SMTP Both]	G	Set Authentication failure event type	switch(config)# event authentication-failure both
event ring-topology-change [Systemlog SMTP Both]	G	Set X-ring topology changed event type	switch(config)# event ring-topology-change both
event systemlog [Link-UP Link-Down Both]	I	Set port event for system log	switch(config)# interface fastethernet 3 switch(config-if)# event systemlog both

event smtp [Link-UP Link-Down Both]	I	Set port event for SMTP	switch(config)# interface fastethernet 3 switch(config-if)# event smtp both
show event	P	Show event selection	switch# show event
no event device-cold-start	G	Disable cold start event type	switch(config)# no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event type	switch(config)# no event authentication-failure
no event X-ring-topology-change	G	Disable X-ring topology changed event type	switch(config)# no event X-ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)# interface fastethernet 3 switch(config-if)# no event systemlog
no event smtp	I	Disable port event for SMTP	switch(config)# interface fastethernet 3 switch(config-if)# no event smtp
show systemlog	P	Show system log client & server information	switch# show systemlog

SNTP Commands Set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)# sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)# sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be	switch(config)# sntp daylight-period 20060101-01:01 20060202-01:01

		applied. Parameter format: [yyyymmdd-hh:mm]	
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)# sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)# sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)# sntp timezone 22
show sntp	P	Show SNTP information	switch# show sntp
show sntp timezone	P	Show index number of time zone list	switch# show sntp timezone
no sntp	G	Disable SNTP function	switch(config)# no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)# no sntp daylight

X-ring Commands Set

Commands	Level	Description	Example
Xring enable	G	Enable X-ring	switch(config)# Xring enable
Xring master	G	Enable ring master	switch(config)# Xring master
Xring couplering	G	Enable couple ring	switch(config)# Xring couplering
Xring dualhoming	G	Enable dual homing	switch(config)# Xring dualhoming
Xring ringport [1st Ring Port] [2nd Ring	G	Configure 1st/2nd Ring Port	switch(config)# Xring ringport 7 8

Port]			
Xring couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)# Xring couplingport 1
Xring controlport [Control Port]	G	Configure Control Port	switch(config)# Xring controlport 2
Xring homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# Xring homingport 3
show Xring	P	Show the information of X - Ring	switch# show Xring
no Xring	G	Disable X-ring	switch(config)# no X ring
no Xring master	G	Disable ring master	switch(config)# no Xring master
no Xring couplering	G	Disable couple ring	switch(config)# no Xring couplering
no Xring dualhoming	G	Disable dual homing	switch(config)# no Xring dualhoming

Web-Based Management

About Web-based Management

The switch has an embedded HTML web site residing in flash memory. This site offers advanced management features and allows the switch to be configured from anywhere on the network.

The web site is designed for Internet Explorer 6.0 and uses Java Applets to reduce bandwidth consumption, enhance access speed, and present an intuitive user interface.

Preparing for Web Management

Before using web management, install the industrial switch on the network and verify that a PC on the local network can connect with the switch through the web browser. The default IP Address, Subnet Mask, Username and Password is listed below:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **root**
- Password: **root**

System Login

1. Launch Internet Explorer on the PC
2. Key in “http:// +” the IP address of the switch”, and then Press “**Enter**”.



3. The login screen will appear
4. Enter the user name and password. The default user name and password are ‘root’
5. Press ‘**Enter**’ or click **OK** button, and then the home screen of the Web-based management appears.



System Information

- **System Name:** A name (64 bytes max) can be assigned to the switch.
- **System Description:** Displays the description of switch. Read only cannot be modified
- **System Location:** A physical location (64 bytes max) can be assigned to the switch.
- **System Contact:** Enter the name of contact person or organization
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)
- Click .

System Information

System Name	<input type="text"/>
System Description	16 10/100TX + 2 10/100/1000T/ Mini-GBIC Combo Managed Swi
System Location	<input type="text"/>
System Contact	<input type="text"/>

Firmware Version	v1.07
Kernel Version	v2.07
MAC Address	000F38013DAB

System information interface

IP Configuration

Configure the IP Settings and DHCP client function

- **DHCP Client:** Used to enable or disable the DHCP client function. When enabled, the switch's IP address is assigned by the network DHCP server. **The default IP address will be replaced by the DHCP server assigned IP address.** After clicking the 'Apply' button, a popup dialog will indicate that the current IP will be lost and the new IP address must be retrieved from the DHCP server.
- **IP Address:** A static IP Address may be assigned. The default IP is 192.168.16.1.
- **Subnet Mask:** Assign the subnet mask of the IP address. This does not have to be done if the DHCP client function is enabled.
- **Gateway:** Assign the network gateway. The default gateway is 192.168.16.254.
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- Click

IP Configuration

DHCP Client :

IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS1	0.0.0.0
DNS2	0.0.0.0

IP configuration interface

DHCP Server – System configuration

The switch can function as a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assignment range.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assignment range.
- **Subnet Mask:** The subnet mask.
- **Gateway:** The network gateway.
- **DNS:** Network Domain Name Server IP Address.
- **Lease Time (sec):** The time interval at which that system will reset the dynamic IP assignment.
- Click

DHCP Server - System Configuration

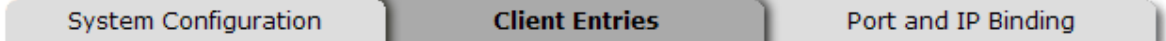
System Configuration	Client Entries	Port and IP Binding
DHCP Server : <input type="button" value="Disable"/>		
Low IP Address	<input type="text" value="192.168.16.100"/>	
High IP Address	<input type="text" value="192.168.16.200"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Gateway	<input type="text" value="192.168.16.254"/>	
DNS	<input type="text" value="0.0.0.0"/>	
Lease Time (sec)	<input type="text" value="86400"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

DHCP Server Configuration interface

DHCP Server – Client Entries

DHCP Client information is displayed.

DHCP Server - Client Entries



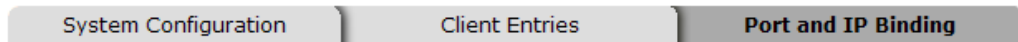
IP addr Client ID Type Status Lease

DHCP Client Entries interface

DHCP Server - Port and IP Bindings

You can assign a specific IP address that is in the dynamic IP assignment range to the specific port. When the device is connected to the port and asks for an assignment, the system will assign this IP address.

DHCP Server - Port and IP Binding



Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0
Port.11	0.0.0.0
Port.12	0.0.0.0
Port.13	0.0.0.0
Port.14	0.0.0.0
Port.15	0.0.0.0
Port.16	0.0.0.0
Port.17	0.0.0.0
Port.18	0.0.0.0

Apply Help

Port and IP Bindings interface

TFTP - Update Firmware

Provides the ability to update the switch's firmware. Before updating, ensure you the TFTP server is ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** Enter the TFTP server IP.
2. **Firmware File Name:** Enter the name of firmware image.
3. Click .

TFTP - Update Firmware

Update Firmware	Restore Configuration	Backup Configuration
TFTP Server IP Address	<input type="text" value="192.168.16.2"/>	
Firmware File Name	<input type="text" value="image.bin"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Update Firmware interface

TFTP – Restore Configuration

If the EEPROM image is stored on the TFTP server, you can restore it to flash memory.

1. **TFTP Server IP Address:** Enter the TFTP server IP.
2. **Restore File Name:** Enter the restore file name.
3. Click .

TFTP - Restore Configuration

Update Firmware	Restore Configuration	Backup Configuration
TFTP Server IP Address	<input type="text" value="192.168.16.2"/>	
Restore File Name	<input type="text" value="data.bin"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Restore Configuration interface

TFTP - Backup Configuration

You can save current EEPROM image to the TFTP server.

1. **TFTP Server IP Address:** Enter the TFTP server IP
2. **Backup File Name:** Enter the file name
3. Click .

TFTP - Backup Configuration

Update Firmware	Restore Configuration	Backup Configuration
TFTP Server IP Address <input type="text" value="192.168.16.2"/>		
Backup File Name <input type="text" value="data.bin"/>		
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Backup Configuration interface

System Event Log – Syslog Configuration

Configure the system event mode to collect system log.

1. **Syslog Client Mode:** Select the system log mode – client only, server only, or both.
2. **System Log Server IP Address:** Assigned the system log server IP
3. Click to refresh the event log.
4. Click to clear all current event log.
5. After configuring, Click .

System Event Log - Syslog Configuration

Syslog Configuration	SMTP Configuration	Event Configuration
----------------------	--------------------	---------------------

Syslog Client Mode	Both	Apply
Syslog Server IP Address	192.168.16.200	

3: Jan 1 00:02:53 : System Log Server IP: 192.168.16.200
2: Jan 1 00:02:53 : System Log Enable!
1: Jan 1 00:02:18 : Clear System Log Table!

Page.1
Page.2
Page.3
Page.4
Page.5
Page.6
Page.7
Page.8
Page.9
Page.10

Page.1

Reload	Clear	Help
--------	-------	------

Syslog Configuration interface

System Event Log - SMTP Configuration

Set up the mail server IP, mail account, account password, and email account for receiving event alerts.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address.
3. **Sender:** Enter the email address, e.g. switch102@123.com, to identify where the event log came from.
4. **Authentication:** Mark the check box to enable and configure the email account and password for authentication.
5. **Mail Account:** set up the email account, e.g. johnadmin for the switch. It must be an existing email account on the mail server.

6. **Password:** The email account password.
7. **Confirm Password:** reconfirm the password.
8. **Rcpt e-mail Address 1 through 6:** Enter up to six email addresses to receive the event log.
9. Click button.

System Event Log - SMTP Configuration

Syslog Configuration	SMTP Configuration	Event Configuration
E-mail Alert: <input type="button" value="Enable"/> <input type="button" value="Disable"/>		
SMTP Server IP Address :	<input type="text" value="192.168.16.5"/>	
Sender :	<input type="text" value="switch101@123.com"/>	
<input checked="" type="checkbox"/> Authentication		
Mail Account :	<input type="text" value="johnadmin"/>	
Password :	<input type="password" value="••••"/>	
Confirm Password :	<input type="password" value="••••"/>	
Rcpt e-mail Address 1 :	<input type="text" value="supervisor@123.com"/>	
Rcpt e-mail Address 2 :	<input type="text"/>	
Rcpt e-mail Address 3 :	<input type="text"/>	
Rcpt e-mail Address 4 :	<input type="text"/>	
Rcpt e-mail Address 5 :	<input type="text"/>	
Rcpt e-mail Address 6 :	<input type="text"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

SMTP Configuration interface

System Event Log - Event Configuration

When the selected events occur, the system will generate a log entry and email notification message. .

- **System event selection:** Four selections available – Cold Start, Warm Start, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When the selected events occur, the system will send the logs.

- **Port event selection:** When a port specific event occurs, the system will generate a log entry and email notification. Three selections are available – Link UP, Link Down, and Link UP & Link Down.

System Event Log - Event Configuration

Syslog Configuration

SMTP Configuration

Event Configuration

System event selection

Event Type	Syslog	SMTP
Device cold start	<input type="checkbox"/>	<input type="checkbox"/>
Device warm start	<input type="checkbox"/>	<input type="checkbox"/>
Authentication Failure	<input type="checkbox"/>	<input type="checkbox"/>
X-Ring topology change	<input type="checkbox"/>	<input type="checkbox"/>

Port event selection

Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
Port.09	Disable	Disable
Port.10	Disable	Disable
Port.11	Disable	Disable
Port.12	Disable	Disable
Port.13	Disable	Disable
Port.14	Disable	Disable
Port.15	Disable	Disable
Port.16	Disable	Disable
Port.17	Disable	Disable
Port.18	Disable	Disable

Apply | Help

Event Configuration interface

Fault Relay Alarm

- **Power Failure:** When the check box is marked, the Fault LED will light if the power source fails.
- **Port Link Down/Broken:** When the check box is marked, the Fault LED will light if a port link goes down.

Fault Relay Alarm

Power Failure	
<input checked="" type="checkbox"/> Power 1	<input checked="" type="checkbox"/> Power 2
Port Link Down/Broken	
<input type="checkbox"/> Port 1	<input type="checkbox"/> Port 2
<input type="checkbox"/> Port 3	<input type="checkbox"/> Port 4
<input type="checkbox"/> Port 5	<input type="checkbox"/> Port 6
<input type="checkbox"/> Port 7	<input type="checkbox"/> Port 8
<input type="checkbox"/> Port 9	<input type="checkbox"/> Port 10
<input type="checkbox"/> Port 11	<input type="checkbox"/> Port 12
<input type="checkbox"/> Port 13	<input type="checkbox"/> Port 14
<input type="checkbox"/> Port 15	<input type="checkbox"/> Port 16
<input type="checkbox"/> Port 17	<input type="checkbox"/> Port 18

Fault Relay Alarm interface

SNTP Configuration

The SNTP allows you to synchronize switch clocks.

1. **SNTP Client:** Enables or disables the SNTP function.
2. **Daylight Saving Time:** Enables or disables daylight saving time. When this function is enabled, the time period must be entered.
3. **UTC Time zone:** Sets the local time zone.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, Russia Zone 1	+2 hours	2 pm
BT - Baghdad, Russia Zone 2	+3 hours	3 pm

ZP4 - Russia Zone 3	+4 hours	4 pm
ZP5 – Russia Zone 4	+5 hours	5 pm
ZP6 - Russia Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, Russia Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, Russia Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** Enter the SNTP server IP address.
5. **Daylight Saving Period:** Enter the Daylight Saving beginning time and Daylight Saving end time.
6. **Daylight Saving Offset (mins):** Enter the offset in minutes.
7. **Switch Timer:** Displays the current time.
8. Click .

SNTP Configuration

SNTP Client : ▾

Daylight Saving Time : ▾

UTC Timezone	<input type="text" value="(GMT+08:00)Taipei"/> ▾	
SNTP Server URL	<input type="text" value="76.168.30.201"/>	
Switch Timer	<input type="text" value="Monday, September 03, 2007 4:35:"/>	
Daylight Saving Period	<input type="text" value="20040101 00:0"/>	<input type="text" value="20040101 00:0"/>
Daylight Saving Offset(mins)	<input type="text" value="0"/>	

SNTP Configuration interface

IP Security

IP security function grants 10 specific IP addresses permission to access the switch through a web browser or TELNET for management.

- **IP Security Mode:** When enabled, allows management via TELNET and HTTP.
- **Enable HTTP Server:** Mark the box to grant the specified IP addresses web based management permission.
- **Enable Telnet Server:** Mark the box to grant the specified IP addresses TELNET management permission.
- **Security IP 1 ~ 10:** Enter up to 10 IP addresses.
- Click

[NOTE] If the configuration is not saved, it will be lost when the switch is powered off.

IP Security

IP Security Mode:

<input type="checkbox"/> Enable HTTP Server
<input type="checkbox"/> Enable Telnet Server

Security IP1	<input type="text" value="0.0.0.0"/>
Security IP2	<input type="text" value="0.0.0.0"/>
Security IP3	<input type="text" value="0.0.0.0"/>
Security IP4	<input type="text" value="0.0.0.0"/>
Security IP5	<input type="text" value="0.0.0.0"/>
Security IP6	<input type="text" value="0.0.0.0"/>
Security IP7	<input type="text" value="0.0.0.0"/>
Security IP8	<input type="text" value="0.0.0.0"/>
Security IP9	<input type="text" value="0.0.0.0"/>
Security IP10	<input type="text" value="0.0.0.0"/>

IP Security interface

User Authentication

Use this function to change the login name and password.

1. **User name:** Enter the new user name (The default is 'root').
2. **Password:** Enter the new password (The default is 'root').
3. **Confirm password:** Confirm the new password.
4. Click

User Authentication

User Name :	<input type="text" value="root"/>
New Password :	<input type="password" value="...."/>
Confirm Password :	<input type="password" value="...."/>

User Authentication interface

Port Statistics

Provides port status.

- **Port:** The port number.
- **Type:** Displays the connection speed.
- **Link:** Displays link status —‘Up’ or ‘Down’.
- **State:** Enabled or Disabled.
- **Tx Good Packet:** Displays the number of good packets transmitted.
- **Tx Bad Packet:** Displays the number of bad packets transmitted.
- **Rx Good Packet:** Displays the number of good packets received.
- **Rx Bad Packet:** Displays the number of bad packets received.
- **Tx Abort Packet:** Displays the number of aborted transmit packets.
- **Packet Collision:** Displays the number of packet collisions.
- **Packet Dropped:** Displays the number of dropped packets.
- **Rx Bcast Packet:** Displays the number of broadcast packets.
- **Rx Mcast Packet:** Displays the number of multicast packets.
- Click button to reset the numbers.

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.15	100TX	Up	Enable	230	0	465	0	0	0	0	5	2
Port.16	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.17	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.18	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Port Statistics interface

Port Control

Used to configure and view port settings.

1. **Port:** Select the port to configure.
2. **State:** Enable or disable the port.
3. **Negotiation:** Set the negotiation status of the port.
4. **Speed:** Set the port link speed.
5. **Duplex:** Set the port to full or half-duplex.
6. **Flow Control:** Set flow control to **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Symmetric**.
7. **Security:** Set the port security. When 'On' is selected, the port will only accept a connection from one MAC address.
8. Click

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01						
Port.02	Enable	Auto	100	Full	Enable	Off
Port.03						
Port.04						

Port	Group ID	Type	Link	State	Negotiation	Speed		Duplex		Flow Control		Security
						Config	Actual	Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.09	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.10	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.11	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.12	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.13	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.14	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.15	N/A	100TX	Up	Enable	Auto	100	Full	100	Full	Enable	ON	OFF
Port.16	N/A	100TX	Down	Enable	Auto	100	Full	N/A	N/A	Enable	N/A	OFF
Port.17	N/A	1GTX/mGBIC	Down	Enable	Auto	1G	Full	N/A	N/A	Enable	N/A	OFF
Port.18	N/A	1GTX/mGBIC	Down	Enable	Auto	1G	Full	N/A	N/A	Enable	N/A	OFF

Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized method for exchanging information between Partner Systems on a link. This allows their Link Aggregation Control instances to reach an agreement on the identity of the Link Aggregation Group, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to four consecutive ports into two dedicated connections. This feature expands bandwidth to a device on the network. **LACP operation requires full-duplex mode.**

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority. It is selected as the active LACP.
2. **Group ID:** There are four trunk groups available. Choose the "**Group ID**" and click
3. **LACP:** If enabled, the group is an LACP static trunk group. If disabled, the group is local static trunk group. All ports support LACP dynamic trunk. If connected to a device that also supports LACP, the LACP dynamic trunk group is automatically created.
4. **Work ports:** A maximum of four ports can be aggregated at the same time. With LACP static trunk group, any excess ports are considered standby and can be aggregated if a work port fails. If it is local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to add to the trunk group. Click button to add the port. To remove unwanted ports, select the port and click button.

6. When LACP enabled, you can configure LACP Active/Passive status for each port on State Activity page.
7. Click
8. Use to delete Trunk Group.

Port Trunk - Aggregator Setting

Aggregator Setting	Aggregator Information	State Activity
System Priority		
<input style="width: 100px;" type="text" value="1"/>		
Group ID	<input style="width: 100px;" type="text" value="Trunk.1"/>	<input type="button" value="Select"/>
Lacp	<input style="width: 100px;" type="text" value="Enable"/>	
Work Ports	<input style="width: 100px;" type="text" value="4"/>	
<div style="border: 1px solid black; padding: 2px;"> Port.01 Port.02 Port.03 Port.04 </div>	<input type="button" value=" <<Add"/> <input type="button" value=" Remove >>"/>	<div style="border: 1px solid black; padding: 2px;"> Port.05 Port.06 Port.07 Port.08 Port.09 Port.10 Port.11 Port.12 Port.13 </div>
<input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>		

Notice: The trunk function do not support GVRP and X-Ring.

Port Trunk—Aggregator setting interface (four ports are added to the left field with LACP enabled)

Aggregator Information

Displays static trunk group information.

Group ID	Trunk.1 ▾	Select
Lacp	Disable ▾	
Work Ports	2	
Port.07 Port.08	<<Add Remove>>	Port.01 ▲ Port.02 Port.03 Port.04 Port.05 Port.06 Port.09 Port.10 Port.11 ▾

Port Trunk—Aggregator setting interface (two ports are added to the left field with LACP disable)

Port Trunk - Aggregator Information

Aggregator Setting

Aggregator Information

State Activity

Static Trunking Group	
Group Key	1
Port Member	7 8

Port Trunk – Aggregator Information interface

State Activity

After setting up the LACP aggregator, port state activity can be configured.

Mark the port and click . The port state activity will change to **Active** or **Passive** depending on its previous state.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port responds only if it receives LACP protocol packets from the opposite device.

-
- [NOTE]**
1. A link having either two active LACP ports or one active port can perform dynamic LACP trunk.
 2. A link, which has two passive LACP ports, will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.
-

Port Trunk - State Activity

Aggregator Setting
Aggregator Information
State Activity

Port	LACP State Activity	Port	LACP State Activity
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active
3	<input checked="" type="checkbox"/> Active	4	<input checked="" type="checkbox"/> Active
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A

Apply
Help

Port Trunk – State Activity interface

Port Mirroring

Port mirroring is a method to monitor traffic in switched networks. Traffic flowing through the indicated ports can be monitored by a specified port.

Port Mirroring

	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.05	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.06	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.07	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.08	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.09	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.10	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.11	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.12	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.13	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.14	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.15	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.16	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.17	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.18	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

Port Trunk – Port Mirroring interface

- **Destination Port:** Only one port can be selected as the destination (mirror) port for monitoring both RX and TX traffic from the source port. Two ports may be configured to monitor RX and TX traffic separately. A LAN analyzer can be connected to the mirror port.
- **Source Port:** Select the ports to monitor. All monitored port traffic will be sent to the mirror (destination) port. Multiple source ports by can be selected by checking the **RX** or **TX** check boxes.
- Click

Rate Limiting

You can set up every port's frame limitation type and bandwidth rate.

Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps
Port.09	All	0 kbps	0 kbps
Port.10	All	0 kbps	0 kbps
Port.11	All	0 kbps	0 kbps
Port.12	All	0 kbps	0 kbps
Port.13	All	0 kbps	0 kbps
Port.14	All	0 kbps	0 kbps
Port.15	All	0 kbps	0 kbps
Port.16	All	0 kbps	0 kbps
Port.17	All	0 kbps	0 kbps
Port.18	All	0 kbps	0 kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate to 1Mbps, and ingress rate is 500Kbps. The switch performs the ingress rate limiting using a packet counter to meet the specified rate
- **Ingress:** Enter the port effective ingress rate(The default value is '0')
- **Egress:** Enter the port effective egress rate(The default value is '0')
- Click

VLAN configuration

A Virtual LAN (VLAN) can be thought of as a broadcast domain that exists within a switch or a defined set of switches. By grouping switch ports into VLANs, traffic flooding is limited since devices can only communicate directly with devices belonging to the VLAN. Creating a VLAN from a switch is the logical equivalent of reconnecting a group of devices to another Layer 2 switch. However, the network devices retain their same physical connection. The switch supports port-based and 802.1Q (tagged-based) VLAN. In the default configuration, the VLAN option is disabled

The switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is “**Disable**”.

VLAN Configuration

VLAN Operation Mode :	Disable
<input type="checkbox"/> Enable GVRP Protocol	
Management Vlan ID :	0

Apply

VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration - Port-based VLAN

With port-based VLAN, the port is assigned to a VLAN. Therefore, all devices attached to a given port should be members of the same VLAN. As with other VLAN configurations, the packets forwarded using this method do not leak into other VLAN domains on the network. After the port has been assigned to a VLAN, devices on the port cannot send to or receive from devices in other VLANs without the intervention of another layer 3 device or the ability to tag the data packet with a specific PVID

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

Management Vlan ID :

Apply

Add Edit Delete Help

VLAN – Port Based interface

- Pull down the selection item for **Port Based** then press button
- Click to add a new VLAN group (64 groups maximum).

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

Management Vlan ID :

Apply

Group Name	<input type="text" value="V_LAN1"/>	
VLAN ID	<input type="text" value="1"/>	
<input type="text" value="Port.05"/> <input type="text" value="Port.06"/> <input type="text" value="Port.07"/> <input type="text" value="Port.08"/> <input type="text" value="Port.09"/> <input type="text" value="Port.10"/> <input type="text" value="Port.11"/> <input type="text" value="Port.12"/> <input type="text" value="Port.13"/> <input type="text" value="Port.14"/> <input type="text" value="Port.15"/> <input type="text" value="Port.16"/>	<input type="button" value="Add"/> <input type="button" value="Remove"/>	<input type="text" value="Port.01"/> <input type="text" value="Port.02"/> <input type="text" value="Port.03"/> <input type="text" value="Port.04"/>

Apply Help

VLAN—Port Based Add interface

VLAN Configuration

VLAN Operation Mode :	Port Based ▾
<input type="checkbox"/> Enable GVRP Protocol	
Management Vlan ID :	0

Apply

V_LAN1___1

Add Edit Delete Help

VLAN—Port Based Edit/Delete interface

- Use **Delete** button to delete the VLAN.
- Use **Edit** button to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

[NOTE] If the configuration is not saved, it will be lost when the port is powered off.

802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification, which allows VLANs to be created across devices from different vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frame. The tag contains a VLAN Identifier (VID).

When the 802.1Q VLAN is enabled, all ports on the switch belong to a default VLAN (VID 1). The default VLAN cannot be deleted. Up to 64 VLAN groups are supported.

802.1Q Configuration

1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port to configure.
3. **Link Type:** there are three link types.
 - **Access Link:** Single switch only. Allows ports to be grouped by setting the same VID.
 - **Trunk Link:** Extended application of **Access Link**. Allows ports to be grouped by setting the same VID on two or more switches.
 - **Hybrid Link:** Both **Access Link** and **Trunk Link**.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

Management Vlan ID : 0

Apply

802.1Q Configuration

Group Configuration

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Apply Help

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	3	
Port.02	Access Link	3	
Port.03	Access Link	3	
Port.04	Access Link	3	
Port.05	Trunk Link	1	6,
Port.06	Trunk Link	1	6,
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	
Port.11	Access Link	1	
Port.12	Access Link	1	
Port.13	Access Link	1	
Port.14	Access Link	1	
Port.15	Access Link	1	
Port.16	Access Link	1	
Port.17	Access Link	1	
Port.18	Access Link	1	

802.1Q VLAN interface

Group Configuration

Edit the existing VLAN Group.

- Select the VLAN group in the table list.
- Click button.

VLAN Configuration

VLAN Operation Mode :	802.1Q
<input type="checkbox"/> Enable GVRP Protocol	
Management Vlan ID :	0

Apply

802.1Q Configuration

Group Configuration

Default	1
VLAN 3	3
VLAN_6	6

Edit Delete

Group Configuration interface

- You can modify the VLAN group name and VLAN ID.

VLAN Configuration

VLAN Operation Mode :	802.1Q
<input type="checkbox"/> Enable GVRP Protocol	
Management Vlan ID :	0

Apply

802.1Q Configuration

Group Configuration

Group Name	VLAN_3
VLAN ID	3

Apply

Group Configuration interface

- Click **Apply** button.

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of Spanning Tree Protocol (STP). It provides a faster spanning tree convergence after a topology change. The switch will auto detect a device that is running STP or RSTP protocol.

RSTP - System Configuration

- After modification, click
- **RSTP mode:** Enable or disable the RSTP.
- **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, the switch must be rebooted. The value must be multiple of 4096.
- **Max Age (6-40):** The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
- **Hello Time (1-10):** The time that controls when, the switch sends out the BPDU packet to check RSTP status. Enter a value between 1 and 10.
- **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning Tree Protocol learning and listening state to the forwarding state. Enter a value between 4 and 30.

[NOTE] Follow this rule to configure the MAX Age, Hello Time, and Forward Delay Time.

$2 \times (\text{Forward Delay Time value} - 1) > \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$

RSTP - System Configuration

System Configuration

Port Configuration

RSTP Mode	Enable ▾
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Apply Help

Root Bridge Information

Bridge ID	0080000F38013DAB
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

RSTP System Configuration interface

RSTP - Port Configuration

Configure path cost and priority of each port.

1. Select the port in Port column.
1. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
2. **Priority:** Network priority. Enter a number between 0 and 240. The value must be a multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabled.

False is P2P disabled.

4. **Edge:** The port directly connected to the end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to 'True' status.
 - **Non STP:** Set **True** to disable STP mathematic calculation. Set **False** to including the STP mathematic calculation.
 - Click .

RSTP - Port Configuration

System Configuration
Port Configuration

Port	Path Cost (1-20000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 ▲ Port.02 ▲ Port.03 ▲ Port.04 ▲ Port.05 ▼	200000	128	Auto ▼	true ▼	false ▼

priority must be a multiple of 16

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	200000	128	True	True	False	Disabled	Disabled
Port.10	200000	128	True	True	False	Disabled	Disabled
Port.11	200000	128	True	True	False	Disabled	Disabled
Port.12	200000	128	True	True	False	Disabled	Disabled
Port.13	200000	128	True	True	False	Disabled	Disabled
Port.14	200000	128	True	True	False	Disabled	Disabled
Port.15	200000	128	True	True	False	Forwarding	Designated
Port.16	200000	128	True	True	False	Disabled	Disabled
Port.17	200000	128	True	True	False	Disabled	Disabled
Port.18	200000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches, hubs, etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

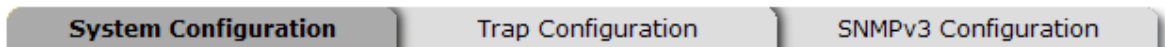
■ Community Strings

Define and remove community strings.

1. **String:** Enter the name of the string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects
4. Click button.
5. To remove the community string, select the community string and click . The default community string cannot be edited.

- **Agent Mode:** Select the SNMP version that you want to use and click

SNMP - System Configuration



Community Strings

Current Strings : Remove	New Community String : Add
public__RO private__RW PString1__RO PString2__RW	String : PString3 <input type="radio"/> RO <input checked="" type="radio"/> RW

Agent Mode

Current Mode: SNMP v1/v2c/v3	<input type="radio"/> SNMP V1/V2C only <input type="radio"/> SNMP V3 only <input checked="" type="radio"/> SNMP V1/V2C/V3
	Change

Help

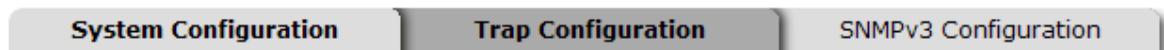
SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives traps (the system alerts generated by the switch). If the trap manager is not defined, traps will not be issued. Create a trap manager by entering the IP address of the station and a community string.

1. **IP Address:** Enter the IP address of the trap manager.
2. **Community:** Enter the community string.
3. **Trap Version:** Select the SNMP trap version type (v1 or v2c).
4. Click **Add**.
5. To remove the community string, select the community and click **Remove**.

SNMP - Trap Configuration



Trap Managers

Current Managers :	New Manager :
<input type="button" value="Remove"/>	<input type="button" value="Add"/>
192.168.16.21: TrapHost1, v1 192.168.16.22: TrapHost2, v2	IP Address : <input type="text" value="192.168.16.23"/> Community : <input type="text" value="TrapHost3"/> Trap version: <input checked="" type="radio"/> v1 <input type="radio"/> v2c

Trap Managers interface

SNMPV3 Configuration

Context Table

Configure SNMP v3 context table. Assign the context name of context table.

Click to add context name. Click to remove the unwanted context name.

User Profile

Configure SNMP v3 user table.

- **User ID:** Enter the user name.
- **Authentication Password:** Enter the authentication password.
- **Privacy Password:** Enter the private password.
- Click to add the context name.
- Click to remove an unwanted context name.

SNMP - SNMPv3 Configuration

System Configuration

Trap Configuration

SNMPv3 Configuration

Context Table	
Context Name :	<input type="text"/> <input type="button" value="Apply"/>

User Table	
Current User Profiles :	New User Profile :
<input type="button" value="Remove"/>	<input type="button" value="Add"/>
(none)	User ID: <input type="text"/>
	Authentication Password: <input type="text"/>
	Privacy Password: <input type="text"/>

Group Table	
Current Group content :	New Group Table:
<input type="button" value="Remove"/>	<input type="button" value="Add"/>
(none)	Security Name (User ID): <input type="text"/>
	Group Name: <input type="text"/>

Access Table	
Current Access Tables :	New Access Table :
<input type="button" value="Remove"/>	<input type="button" value="Add"/>
(none)	Context Prefix: <input type="text"/>
	Group Name: <input type="text"/>
	Security Level: <input type="radio"/> NoAuthNoPriv. <input type="radio"/> AuthNoPriv. <input type="radio"/> AuthPriv.
	Context Match Rule <input type="radio"/> Exact <input type="radio"/> Prefix
	Read View Name: <input type="text"/>
	Write View Name: <input type="text"/>
	Notify View Name: <input type="text"/>


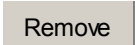
MIBView Table	
Current MIBTables :	New MIBView Table :
<input type="button" value="Remove"/>	<input type="button" value="Add"/>
(none)	View Name: <input type="text"/>
	SubOid-Tree: <input type="text"/>
	Type: <input type="radio"/> Excluded <input type="radio"/> Included

Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

SNMP V3 configuration interface


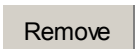
Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you set up in the user table.
- **Group Name:** Set up the group name.
- Click  to add the context name.
- Click  to remove an unwanted context name.


Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click  to add the context name.
- Click  to remove an unwanted context name.

MIBview Table

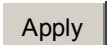
Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type—excluded or included.
- Click  to add the context name.

- Click  to remove an unwanted context name.

QoS Configuration

QoS Policy and Priority Type

- **QoS Policy:** select the QoS policy rule.
 - **Use an 8,4,2,1 weighted fair queuing scheme:** The switch will follow 8:4:2:1 rate to process the priority queue from the highest to the lowest queue. For example, when processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time.
 - **Use the strict priority scheme:** The highest queue will always be processed first.
- **Priority Type:** there are five priority selections available.
- **Port-base:** the port priority will follow the assigned **Port-base** – High, middle, low, or lowest.
 - **COS Only:** the port priority will only follow the **COS priority** assigned.
 - **TOS only:** the port priority will only follow the **TOS priority** assigned.
 - **COS first:** the port priority will follow the COS priority first, and then the other priority rule.
 - **TOS first:** the port priority will follow the TOS priority first, and then the other priority rule.
- Click .

QoS Configuration

Qos Policy:

Use an 8,4,2,1 weighted fair queuing scheme
 Use a strict priority scheme
 Priority Type:

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08
<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Port.09	Port.10	Port.11	Port.12	Port.13	Port.14	Port.15	Port.16
<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Port.17	Port.18						
<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>						

COS:

Priority	0	1	2	3	4	5	6	7
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>

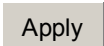
TOS:

Priority	0	1	2	3	4	5	6	7
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	8	9	10	11	12	13	14	15
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	16	17	18	19	20	21	22	23
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	24	25	26	27	28	29	30	31
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	32	33	34	35	36	37	38	39
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	40	41	42	43	44	45	46	47
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	48	49	50	51	52	53	54	55
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>
Priority	56	57	58	59	60	61	62	63
	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>	<input type="text" value="Lowest"/>

QoS Configuration interface

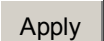
Port-based Priority

- **Port x:** Each port has 4 priority levels—High, Middle, Low, and Lowest—to select from.

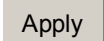
- Click  button to make the settings effective.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0 to 7 –High, Middle, Low, Lowest.
- Click .

TOS Configuration

- **TOS priority:** the system provides 0 to 63 TOS priority levels. Each level has four types of priority – high, middle, low, and lowest. The default value is 'Lowest'. When an IP packet is received, the system will check the TOS level value in the IP packet. For example, if the TOS level 25 is high and the port is following the TOS priority policy only, when a packet is received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), then the packet will have highest priority.
- Click  button to make the settings effective.

IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of message.

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

Enable IGMP protocol on the web management switch setting advanced page. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function (Enable or Auto) to set the switch as a querier for an IGMP version 2 multicast network.
- Click button.

IGMP Configuration

IP Address	VLAN ID	Member Port
239.255.255.250	1	*****15***

IGMP Snooping:

IGMP Query:

IGMP Configuration interface

X-Ring

X-Ring provides network redundancy similar to the Spanning Tree and Rapid Spanning Tree Protocols. However, recovery time is greatly reduced when the X-Ring protocol is used. The protocol identifies one switch as the Ring Master. Packets are blocked from the redundant path unless a ring member becomes disconnected from the rest of the network. When this happens, the protocol automatically restores connectivity using the redundant path.

In the X-Ring topology, every switch should enable X-Ring function and assign two member ports to the ring. Only one switch in the X-Ring group would be set as the backup switch. Other switches are called working switches and their two member ports are called working ports. If a network connection failure occurs, the backup port will automatically become a working port to recover.

The switch can be set in the ring master or slave mode. The ring master negotiates and places commands to the other switches in the X-Ring group. If there are two or more switches in the master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master mode is enabled using the X-Ring configuration interface. The Ring Master can also be identified using the R.M. LED on the front of the switch.

The switch also supports coupling ring to connect two or more X-Ring groups for redundant backup. The dual homing function is used to prevent a connection lose between the X-Ring group and the upper level/core switch.

- **Enable X-Ring:** Mark the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box to set the switch as the Ring Master.
- **1st & 2nd Ring Ports:** Assign two ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.

- **Enable Coupling Ring:** Mark the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port.
- **Control port:** Set the switch as the master switch in the coupling ring.

Enable Dual Homing: Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, only one port can be the Dual Homing port. Dual Homing only works when the X-Ring function is enabled.

- Click .

X-Ring Configuration

<input checked="" type="checkbox"/> Enable Ring		
<input type="checkbox"/> Enable Ring Master		
1st Ring Port	Port.01 ▾	LINKDOWN
2nd Ring Port	Port.02 ▾	LINKDOWN
<input type="checkbox"/> Enable Couple Ring		
Couple Port	Port.03 ▾	LINKDOWN
Control Port	Port.04 ▾	LINKDOWN
<input type="checkbox"/> Enable Dual Homing		
Homing Port	Port.05 ▾	LINKDOWN
<input type="checkbox"/> Enable Central Ring 1		
1st Ring Port	Port.09 ▾	LINKDOWN
2nd Ring Port	Port.10 ▾	LINKDOWN
<input type="checkbox"/> Enable Central Ring 2		
1st Ring Port	Port.11 ▾	LINKDOWN
2nd Ring Port	Port.12 ▾	LINKDOWN
<input type="checkbox"/> Enable Central Ring 3		
1st Ring Port	Port.13 ▾	LINKDOWN
2nd Ring Port	Port.14 ▾	LINKDOWN
<input type="checkbox"/> Enable Central Ring 4		
1st Ring Port	Port.15 ▾	LINKDOWN
2nd Ring Port	Port.16 ▾	FORWARDING

X-ring Interface

-
- [NOTE]**
1. When the X-Ring function is enabled, disable RSTP.
 2. If the configuration is not saved, it will be lost when the switch is powered off.
-

Security

802.1X/RADIUS Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it proves authority by providing a user name and password, which is verified by a separate server.

System Configuration

1. **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
2. **Radius Server IP:** Enter the Radius Server IP address.
3. **Server Port:** Enter the UDP destination port for authentication requests to the Radius Server.
4. **Accounting Port:** Enter the UDP destination port for accounting requests to the Radius Server.
5. **Shared Key:** Enter an encryption key for use during authentication sessions. This key must match the encryption key used on the Radius Server
6. **NAS, Identifier:** Enter the identifier of the radius client.
7. Click

802.1x/RADIUS - System Configuration

System Configuration	Port Configuration	Misc Configuration
802.1x Protocol	Disable ▾	
Radius Server IP	0.0.0.0	
Server Port	1812	
Accounting Port	1813	
Shared Key	12345678	
NAS, Identifier	NAS_L2_SWITCH	

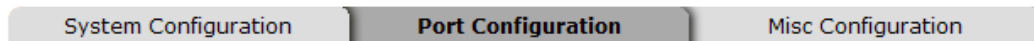
802.1x System Configuration interface

802.1x Port Configuration

You can configure 802.1x authentication state for each port. The State choices are Disable, Accept, Reject and Authorize. Use the 'Space' key change the state value.

- **Reject:** The port is held in the unauthorized state.
- **Accept:** The port is held in the Authorized state.
- **Authorized:** The port will allow an authentication exchange between the supplicant and the authentication server.
- **Disable:** The port is held in the Authorized state
- Click .

802.1x/Radius - Port Configuration



Port	State
Port.01	Authorize
Port.02	Reject
Port.03	Accept
Port.04	Authorize
Port.05	Disable

Port Authorization

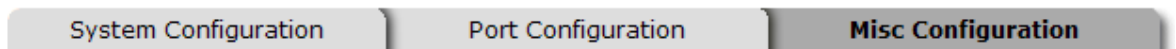
Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable
Port.11	Disable
Port.12	Disable
Port.13	Disable
Port.14	Disable
Port.15	Disable
Port.16	Disable
Port.17	Disable
Port.18	Disable

802.1x Per Port Setting interface

Misc Configuration

- **Quiet Period:** Sets the period during which the port does not try to acquire a supplicant.
- **TX Period:** Sets the period that the port waits before retransmitting the next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Sets the period the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period the switch waits for a server response to an authentication request.
- **Max Requests:** Sets the number of authentications that time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time after which connected clients must be re-authenticated.
- Click .

802.1x/Radius - Misc Configuration



Quiet Period	<input type="text" value="60"/>
Tx Period	<input type="text" value="30"/>
Supplicant Timeout	<input type="text" value="30"/>
Server Timeout	<input type="text" value="30"/>
Max Requests	<input type="text" value="2"/>
Reauth Period	<input type="text" value="3600"/>

802.1x Misc Configuration interface

MAC Address Table



Use the MAC address table to ensure the port security.

Static MAC Address

You can add a static MAC address. This address remains in the switch's address table, regardless of whether the device is physically connected to the switch. Therefore, the switch does not have to re-learn a device's MAC address when the disconnected or powered-off device reconnects to the network. You can add / modify / delete a static MAC address.

Add the Static MAC Address

You can add static MAC address in the switch MAC table here.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** Pull down the selection menu to select the port number.
- Click  button.
- If you want to delete the MAC address from filtering table, select the MAC address and click  button.

MAC Address Table - Static MAC Address

Static MAC Addresses	MAC Filtering	All Mac Addresses				
<table border="1"><thead><tr><th>MAC Address</th><th>Port No.</th></tr></thead><tbody><tr><td>AABBCCDDEEFF</td><td>Port.01</td></tr></tbody></table>			MAC Address	Port No.	AABBCCDDEEFF	Port.01
MAC Address	Port No.					
AABBCCDDEEFF	Port.01					
<table border="1"><tr><td>MAC Address</td><td><input type="text" value="FFEEDDCCBBAA"/></td></tr><tr><td>Port No.</td><td><input type="text" value="Port.01"/></td></tr></table>			MAC Address	<input type="text" value="FFEEDDCCBBAA"/>	Port No.	<input type="text" value="Port.01"/>
MAC Address	<input type="text" value="FFEEDDCCBBAA"/>					
Port No.	<input type="text" value="Port.01"/>					
<p><input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Help"/></p>						

Static MAC Addresses interface

MAC Filtering

MAC Address Table - MAC Filtering

Static MAC Addresses	MAC Filtering	All Mac Addresses		
<table border="1"><thead><tr><th>MAC Address</th></tr></thead><tbody><tr><td>EEFFDDCCBBAA</td></tr></tbody></table>			MAC Address	EEFFDDCCBBAA
MAC Address				
EEFFDDCCBBAA				
<table border="1"><tr><td>MAC Address</td><td><input type="text" value="BBAACDDFFEE"/></td></tr></table>			MAC Address	<input type="text" value="BBAACDDFFEE"/>
MAC Address	<input type="text" value="BBAACDDFFEE"/>			
<p><input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Help"/></p>				

MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. Click button.
3. If you want to delete the MAC address from the filtering table, select the MAC address and click button.

All MAC Addresses

You can view the port that connected device's MAC address and the related devices' MAC address.

1. Select the port.
2. The selected port static & dynamic MAC address information will be displayed.
3. Click to clear the port static MAC address.

MAC Address Table - All Mac Addresses

The screenshot shows the 'All Mac Addresses' tab selected in a navigation bar. Below the navigation bar, there is a 'Port No:' dropdown menu set to 'Port.01'. A table displays the MAC address 'AABBCCDDEEFF' with the type 'STATIC'. Below the table, the counts are shown: 'Dynamic Address Count:0' and 'Static Address Count:1'. At the bottom, there is a 'Clear MAC Table' button.

All MAC Address interface

Factory Default

To reset switch to the default configuration, click . This function has the option of retaining the current IP address and username/password.

Factory Default

- Keep current IP address setting?
- Keep current username & password?

Factory Default interface

Save Configuration

Click to save the configuration to the flash memory.

Save Configuration

Save Configuration interface

System Reboot

Click to reboot the system.

System Reboot

Please click **[Reboot]** button to restart switch device.

System Reboot interface

Trouble shooting

- Verify that 12 to 48VDC power is available. Do not exceed 48VDC.
- Select the proper cable to construct your network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections:

100Ω Category 3, 4, or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps, or 100Ω Category 5e/above cable for 1000Mbps connections. Ensure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **LED Indicators:** The LEDs can be used to diagnose system problems

Technical Specification

Standard	<p>IEEE 802.3 10Base-T</p> <p>IEEE 802.3u 100Base-TX</p> <p>IEEE 802.3ab 1000Base-T</p> <p>IEEE 802.3z Gigabit fiber</p> <p>IEEE 802.3x Flow Control and Back-pressure</p> <p>IEEE 802.3ad Port trunk with LACP</p> <p>IEEE 802.1d Spanning Tree</p> <p>IEEE 802.1w Rapid Spanning Tree</p> <p>IEEE 802.1p Class of Service</p> <p>IEEE 802.1Q VLAN Tag</p> <p>IEEE 802.1x User Authentication (RADIUS)</p>
Protocol	CSMA/CD
Transfer Rate	<p>14,880 pps for 10Base-T Ethernet port</p> <p>148,800 pps for 100Base-TX/FX Fast Ethernet port</p> <p>1,488,000 pps for Gigabit Fiber Ethernet port</p>
MAC address	8K MAC address table
Packet Buffer	1Mbits
LED	<p>Per unit: Power (Green), Power 1 (Green), Power 2 (Green), Fault (Red), Master (Green)</p> <p>16 10/100TX: Link/Activity (Green), Full duplex/Collision (Yellow)</p> <p>Gigabit Copper: Link/Activity (Green), Speed (1000M Green)</p> <p>SFP: Link/Activity (Green)</p>
Network Cable	<p>10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m)</p> <p>100Base-TX: 2-pair UTP/STP Cat. 5 cable EIA/TIA-568 100-ohm (100m)</p>

	1000Base-T: 2-pair UTP/STP Cat. 5e or 6 cable EIA/TIA-568 100-ohm (100m)
Optical cable	<ul style="list-style-type: none"> ■ LC (Multi-mode): 50/125um or 62.5/125um ■ LC (Single mode): 9/125um
Back-plane	7.2Gbps
Packet throughput ability	10.7Mpps at 64bytes
Power Supply	12 to 48 VDC Redundant power with reverse polarity protection and removable terminal block
Power Consumption	11.2 Watts
Install	DIN Rail and Wall Mount Design
Operation Temp.	-40°C to 75°C
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40°C to 85°C
Case Dimension	IP-30, 72 mm (W) x 105 mm (D) x 152mm (H)
EMI	FCC Class A CE EN61000-4-2 (ESD) CE EN61000-4-3 (RS) CE EN61000-4-4 (EFT) CE EN61000-4-5 (Surge) CE EN61000-4-6 (CS) CE EN61000-4-8

	CE EN61000-4-11 CE EN61000-4-12 CE EN61000-6-2 CE EN61000-6-4
Safety	CE/EN60950-1
Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)